Instituto Politécnico de Tomar

Escola Superior de Tecnologia de Tomar

Engenharia Informática

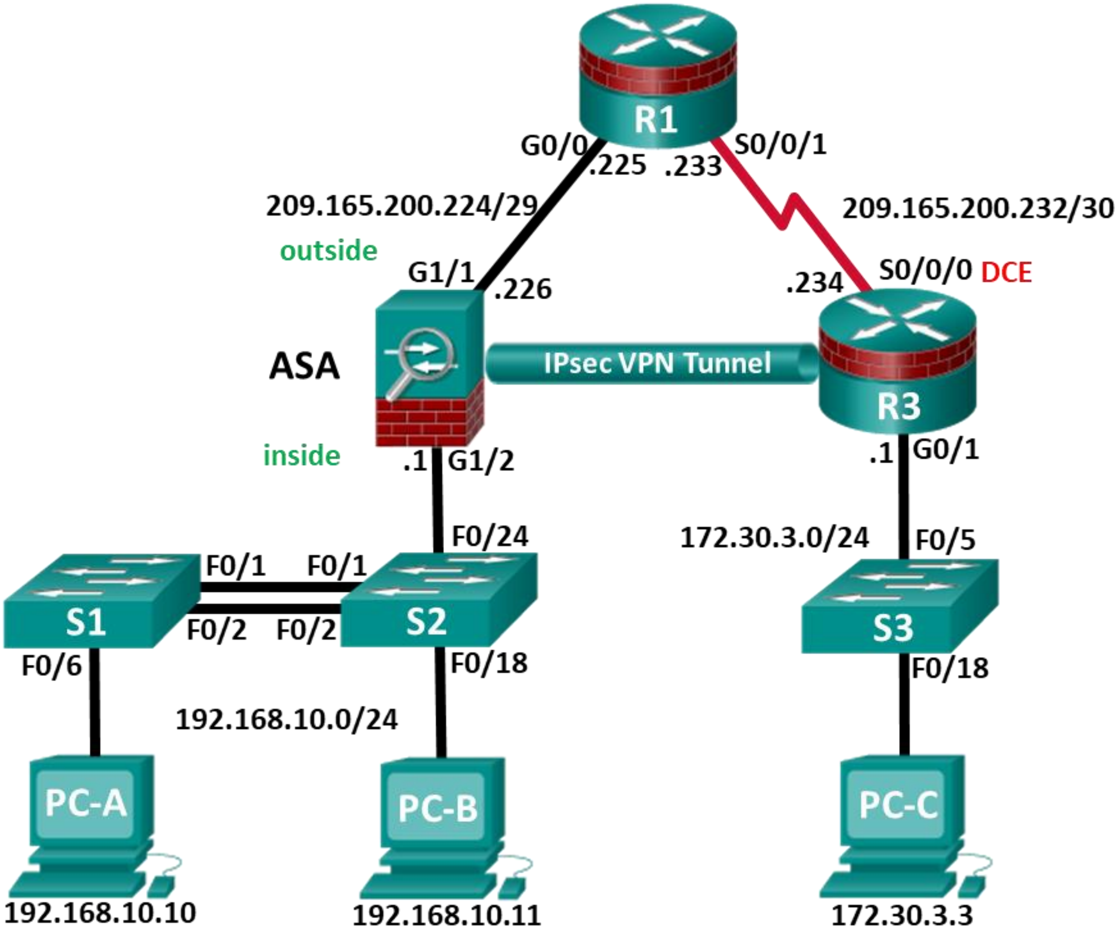
Redes de Dados II

2021 / 2022

Trabalho Laboratorial 3:

Based on Cisco CCNA lab guide.

Topology



Assessment Objectives

Part 1: Verify Network Connectivity (1 points, 5 minutes**)**

Part 2: Configure Secure Router Administrative Access (17 points, 15 minutes)

Part 3: Configure a Zone-Based Policy Firewall (14 points, 10 minutes)

Part 4: Secure Layer 2 Switches (22 points, 20 minutes)

Part 5: Configure ASA Basic Management and Firewall Settings (18 points, 15 minutes)

Part 6: Configure a Site-To-Site IPsec VPN (28 points, 25 minutes)

Scenario

This Skills Assessment (SA) is the final practical exam of student training for the CCNA Security course. The exam is divided into six parts. The parts should be completed sequentially and signed off by your instructor before moving on to the next part. In Part 1 you will verify that the basic device settings have been preconfigured by the instructor. In Part 2, you will secure a network router using the command-line interface (CLI) to configure various IOS features including AAA and SSH. In Part 3, you will configure zone-based policy firewall (ZPF) on an integrated service router (ISR) using the CLI. In Part 4, you will configure and secure Layer 2 switches using the CLI. In Part 5, you will configure the ASA management and firewall settings using the CLI. In Part 6, you will configure a site-to-site IPsec VPN between R3 and the ASA using the CLI and ASDM.

Required Resources

- 2 Routers (Cisco 1941 with Cisco IOS Release 15.4(3)M2 image with a Security Technology Package license)
- 3 Switches (Cisco 2960 with cryptography IOS image for SSH support – Release 15.0(2)SE7 or comparable)
- 1 ASA 5506-X (OS version 9.10(1) and ASDM version 7.10(1) and Base license or comparable)
- 3 PCs (Windows, SSH Client and Java version compatible with installed ASDM version)
- Console cable to configure the Cisco IOS devices via the console ports
- Ethernet and Serial cables as shown in the topology

Part 1: Verify Network Connectivity

Total points: 17

Time: 15 minutes

In the interest of time, your instructor has pre-configured basic settings on R1 and R3, and the static IP address information for the PC hosts in the topology. In Part 1, you will verify that PC-C can ping the G0/1 interface on R3.

Configuration Task	Specification
Ping the G0/1 interface on R3 from PC-C.	See Topology for specific settings.
Ping the S0/0/1 interface on R1 from R3.	See Topology for specific settings.

Instructor Sign-Off Part 1: ______________________

Points: _________ **of 1**

Note: Do not proceed to Part 2 until your instructor has signed off on Part 1.

Part 2: Configure Secure Router Administrative Access

Total points: 17

Time: 15 minutes

In Part 2, you will secure administrative access on router R3 using the CLI. Configuration tasks include the following:

Configuration Item or Task	Specification
Set minimum password length.	Minimum Length: **10** characters
Assign and encrypt a privileged EXEC password.	Password: **cisco12345** Encryption type: 9 (**scrypt**)
Add a user in the local database for administrator access	Username: **Admin01** Privilege level: **15** Encryption type: 9 (**scrypt**) Password: **admin01pass**
Configure MOTD banner.	**Unauthorized Access is Prohibited!**
Disable HTTP server services.	
Configure SSH.	Domain name: **ccnassecurity.com** RSA Keys size: **1024** Version: **2** Timeout: **90** seconds Authentication retries: **2**
Configure VTY lines to allow SSH access.	Allow only **SSH** access.
Configure AAA authentication and authorization settings.	Enable AAA Use **local database** as default setting.
Configure NTP.	Authentication Key: **NTPpassword** Encryption: **MD5** Key: **1** NTP Server: **209.165.200.233** Configure for periodic calendar updates.
Configure syslog.	Enable timestamp service to log the date and time in milliseconds. Send syslog messages to: **172.30.3.3** Set message logging severity level: **Warnings**

Note: Before proceeding to Part 3, ask your instructor to verify R3’s configuration and functionality.

Instructor Sign-Off Part 2: ______________________

Points: _________ of 17

Part 3: Configure a Zone-Based Policy Firewall

Total points: 14

Time: 10 minutes

In Part 3, you will configure a zone-based policy firewall on R3 using the CLI. Configuration tasks include the following:

Configuration Item or Task	Specification
Create security zone names.	Inside zone name: **INSIDE** Outside zone name: **INTERNET**
Create an inspect class map.	Class map name: **INSIDE_PROTOCOLS** Inspection type: **match-any** Protocols allowed: **tcp, udp, icmp**
Create an inspect policy map.	Policy map name: **INSIDE_TO_INTERNET** Bind the class map to the policy map. Matched packets should be inspected.
Create a zone pair.	Zone pair name: **IN_TO_OUT_ZONE** Source zone: **INSIDE** Destination zone: **INTERNET**
Apply the policy map to the zone pair.	Zone pair name: **IN_TO_OUT_ZONE** Policy map name: **INSIDE_TO_INTERNET**
Assign interfaces to the proper security zones.	Interface G0/1: **INSIDE** Interface S0/0/0: **INTERNET**

Troubleshoot as necessary to correct any issues discovered.

Note: Before proceeding to Part 4, ask your instructor to verify your ZPF configuration and functionality.

Instructor Sign-Off Part 2: ______________________

Points: _________ **of 14**

Part 4: Secure Layer 2 Switches

Total points: 22

Time: 20 minutes

Note: Not all security features in this part of the exam will be configured on all switches. However, in a production network, all security feature will be configured on all switches. In the interest of time, the security features are configured on just S2, except where noted.

In Part 4, you will configure security settings on the indicated switch using the CLI. Configuration tasks include the following:

Configuration Item or Task	Specification
Assign and encrypt a privileged EXEC password.	Switch: **S2** Password: **cisco12345**. Encryption type: 9 (**scrypt**)
Add a user in the local database for administrator access	Switch: **S2** Username: **Admin01** Privilege level: **15** Encryption type: 9 (**scrypt**) Password: **admin01pass**
Configure MOTD banner.	Switch: **S2** Banner: **Unauthorized Access is Prohibited!**
Disable HTTP and HTTP secure server.	Switch: **S2**
Configure SSH.	Switch: **S2** Domain name: **ccnassecurity.com** RSA Keys size: **1024** Version: **2** Timeout: **90** seconds Authentication retries: **2**
Configure VTY lines to allow SSH access.	Switch: **S2** Allow **SSH** access only.
Configure AAA authentication and authorization settings.	Switch: **S2** Enable **AAA** Use **local database** as default setting
Create VLAN list.	Switches: **S1 & S2** VLAN**: 2,** Name: **NewNative** VLAN: **10**, Name: **LAN** VLAN: **99**, Name: **Blackhole**
Configure trunk ports.	Switches: **S1 & S2** Interfaces: **F0/1, F0/2** Native VLAN: 2 Prevent DTP.
Disable trunking.	Switch: **S2** Ports: **F0/18, F0/24** VLAN assignment: **10**
Enable PortFast and BPDU guard.	Switch: **S2** Ports: **F0/18, F0/24**

Configuration Item or Task	Specification
Configure basic port security.	Switch: **S2** Port: **F0/18** Maximum limit: **1** Remember MAC Address Violation Action: **Shutdown**
Disable unused ports on S2, and assign ports to VLAN 99.	Switch: **S2** Ports: **F0/3-17, F0/19-23, G0/1-2**
Configure Loop guard.	Switch: **S2** Loop guard: **Default**
Configure DHCP snooping.	Enable DHCP Snooping globally Enable DHCP for VLAN: **10** DHCP trusted interface: **F0/24**

NETLAB+ Note: Use a Maximum limit of **2** when configuring basic port security. Otherwise, the hidden Control Switch will cause a violation to occur and the port will be shutdown.

Troubleshoot as necessary to correct any issues discovered.

Note: Before proceeding to Part 5, ask your instructor to verify your switch configuration and functionality.

Instructor Sign-Off Part 4: ______________________

Points: _________ of 22

Part 5: Configure ASA Basic Management and Firewall Settings

Total points: 18

Time: 15 minutes

Note: By default, the privileged EXEC password is blank. Press **Enter** at the password prompt.

In Part 5, you will configure the ASA's basic setting and firewall using the CLI. Configuration tasks include the following:

Configuration Item or Task	Specification
Configure the ASA hostname.	Name: **CCNAS-ASA**
Configure the domain name.	Domain Name: **ccnasecurity.com**
Configure the privileged EXEC password.	Password: **cisco12345**
Add a user to the local database for administrator console access.	User: **Admin01** Password: **admin01pass**
Configure AAA to use the local database for SSH user authentication for console access.	
Configure interface G1/2.	Name: **inside** IP address: **192.168.10.1** Subnet Mask: **255.255.255.0** Security Level: **100**
Configure interface G1/1.	Name: **outside** IP address: **209.165.200.226** Subnet Mask: **255.255.255.248** Security Level: **0** Activate the VLAN
Generate an RSA key pair to support the SSH connections.	Key: **RSA** Modulus size: **1024**
Configure ASA to accept SSH connections from hosts on the inside LAN.	Inside Network: **192.168.10.0/24** Timeout: **10** minutes Version: **2**
Configure the default route.	Default route IP address: **209.165.200.225**
Configure ASDM access to the ASA.	Enable HTTPS server services. Enable HTTPS on the inside network.
Create a network object to identify internal addresses for PAT. Bind interfaces dynamically by using the interface address as the mapped IP.	Object name: **INSIDE-NET** Subnet: **192.168.10.0/24** Interfaces: **inside, outside**
Modify the default global policy to allow returning ICMP traffic through the firewall.	Policy-map: **global_policy** Class: **inspection_default** Inspect: **icmp**

Troubleshoot as necessary to correct any issues discovered.

Note: Before proceeding to Part 6, ask your instructor to verify your ASA configuration and functionality.

Instructor Sign-Off Part 5: ______________________

Points: _________ of 18

Part 6: Configure a Site-to-Site VPN

Total points: 28

Time: 25 minutes

In Part 6, you will configure a Site-to-Site IPsec VPN between R3 and the ASA. You will use the CLI to configure R3 and use ASDM to configure the ASA.

Step 1: Configure Site-to-Site VPN on R3 using CLI.

Configuration parameters include the following:

Configuration Item or Task	Specification
Enable IKE.	
Create an ISAKMP policy.	ISAKMP Policy Priority: **1** Authentication type: **pre-share** Encryption: **3des** Hash algorithm: **sha** Diffie-Hellman Group Key Exchange: **2**
Configure the pre-shared key.	Preshare key: **ciscopreshare** Address: **209.165.200.226**
Configure the IPsec transform set.	Tag: **TRNSFRM-SET** ESP transform: **ESP_3DES** Hash function: **ESP_SHA_HMAC**
Define interesting traffic.	ACL: **101** Source Network: **172.30.3.0 0.0.0.255** Destination Network: **192.168.10.0 0.0.0.255**
Create a crypto map.	Crypto map name: **CMAP** Sequence number: **1** Type: **ipsec-isakmp** ACL to match: **101** Peer: **209.165.200.226** Transform-set: **TRNSFRM-SET**
Apply crypto map to the interface.	Interface: **S0/0/0** Crypto map name: **CMAP**

Step 2: Configure Site-to-Site VPN on ASA using ASDM

Use a browser on PC-B to establish an ASDM session to the ASA. When the session is established, use the **Site-to-Site VPN Wizard** to configure the ASA for IPsec Site-to-Site VPN. Configuration parameters include the following:

Configuration Item or Task	Specification
Use a browser on PC-B, connect to the ASA, and run ASDM.	Connection: **HTTPS** IP Address: **192.168.10.1** Username: **Admin01** Password: **admin01pass** **Note:** You will need to accept all security messages.
Use the Site-to-site VPN Wizard to configure the site-to-site VPN settings on the ASA.	Peer IP Address: **209.165.200.234** VPN Access Interface: **outside** Local Network: **inside-network/24** Remote Network: **172.30.3.0/24** Pre-shared Key: **ciscopreshare** Exempt ASA side/host network from NAT: **Enable**
Ping PC-B from PC-C.	This should generate interesting traffic and start site-to-site VPN.
Ping PC-C from PC-B.	
Display the ISAKMP and IPsec SAs on R3.	
Verify that a site-to-site session has been established using ASDM from PC-B.	

Troubleshoot as necessary to correct any issues discovered.

Instructor Sign-Off Part 6: ______________________

Points: _________ **of 28**

Router Interface Summary

Router Interface Summary				
Router Model	**Ethernet Interface #1**	**Ethernet Interface #2**	**Serial Interface #1**	**Serial Interface #2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/0/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.